REMARKS

In an Advisory Action mailed April 18, 2007, the Examiner indicated that the claim amendments would not be entered as they raise new issues. Accordingly, this Amendment accompanies a Request for Continued Examination (RCE), resubmitting the claims amendments and arguments.

Claims 1-4, 6-10, 12-15, 17-36, 42, 44-59, and 61-68 were examined in the Final Office Action.

Claim 1 is now amended to include the limitations of dependent claims 2-4, 7 and 8, which are cancelled above. No new limitations are being added, and claims 2-4, 7, and 8 have already been examined. Claim 34 is amended to address an indefiniteness rejection. After entry of the Amendment, claims 1, 6, 9, 10, 12-15, 17-36, 42, 44-59, and 61-68 are submitted for consideration by the Examiner. Withdrawal of the rejections and/or objections are respectfully requested.

A. Rejections under 35 U.S.C §112

The Office Action rejected claim 34 as being indefinite due to lack of antecedent basis for the limitation "regular expressions." Claim 34 is amended to address this rejection by deletion of the term "regular" from the claim.

B. Anticipation Rejections under 35 U.S.C. §102

The Office Action rejected claims 55-59 and 61 under 35 U.S.C. §102(b) as anticipated by U.S. Pat. No. 5,832,212 ("*Cragun*"). This rejection is traversed based on the following remarks.

Claim 55 is directed to a method for monitoring and maintaining an use policy for computer network usage in which TCP/IP data is first captured on a network. Significantly, the method of claim 55 calls for "removing data content that does not contain language elements and storing a remaining content comprising a string of language elements separated by spaces without regard to original formatting of the captured TCP/IP data." After this normalization function is performed on the captured network data the remaining content is protocol and data format independent, which allows later processing using generic patterns

that are protocol and document independent (e.g., the "predetermined expressions" used in the testing step do not have to be configured to be useful with specific communication protocols or specific document or data formatting). The generation of such normalized data or "remaining content" is not shown or suggested by *Cragun*, and Applicant requests that the anticipation rejection be withdrawn (and as discussed in the prior Amendment, such processing is not shown or suggested in the other references cited by the Examiner).

Specifically, the Office Action cites *Cragun* at col. 5, line 35 to col. 6, line 30 as teaching the step of "removing data content...and storing a remaining content comprising a string of language elements separated by spaces without regard to original formatting of the capture TCP/IP data." Applicant has studied the cited portion of *Cragun* and found no discussion of removing data content or of storing remaining content as called for in the claim. The usefulness of such a normalization step is described in Applicant's specification beginning at page 5, line 17. Instead of such normalization, *Cragun* simply teaches that each data packet (col. 5, line 5, line 18) is checked "character-by-character" (col. 5, line 47) for finding particular words or word fragments that are to be "censored" (e.g., by being replaced by a number of symbols such as asterisks or the like). Identified words or word fragments are marked for censoring according to user set rules. The data packet is not logged or stored unless a particular threshold is surpassed. Hence, *Cragun* fails to show processing captured data from a network to normalize it into a string of language elements separated by spaces regardless of its protocol and also fails to show storing such a processed data as "remaining content." As a result, *Cragun* cannot be said to anticipate the removing data content and storing a remaining content step of claim 55, and the rejection should be withdrawn.

Further, because *Cragun* fails to teach removing any data content from its data packets, the reference further fails to teach or suggest the step of "testing the remaining content for the presence of predetermined expressions." *Cragun* suggests testing an entire data packet character-by-character for words or word fragments that are to be censored and not a subset of a captured set of TCP/IP data. Similarly, *Cragun* also fails to teach "storing the remaining data" when a

sum of values exceeds a threshold value because it teaches at the cited col. 4, lines 35-55 that if a log threshold is exceeded "then current information with transmission statistics is stored as indicated at a block 314." Hence, *Cragun* teaches that the entire data packet or current information is stored along with other statistics and does not teach storing only the remaining content (i.e., captured TCP/IP data that has been normalized) as called for in claim 55. As a result, *Cragun* does not anticipate each and every claim limitation as required under 35 U.S.C. §102 because it fails to teach the removing step, the testing step, and the storing step of the claim.

Claims 56-59 and 61 depend from claim 55 and are believed allowable over *Cragun* for at least the reasons provided for allowing claim 55 over this reference. Further, claim 56 calls for the remaining data to only be stored if the sum exceeds the threshold value in a plurality of categories. Again, *Cragun* fails to discuss creating a remaining data set and cannot teach storing such a data set. Further, *Cragun* does not teach storing its data packet or current information only when the sum exceeds threshold values for a plurality of categories but instead teaches storing current information when "the" log threshold is exceeded (see, col. 4, lines 51-55). The Office Action cites *Cragun* for its teaching of a super category at col. 8, lines 15-39, but super categories 820 are shown in Figure 15 and described in the cited portion without any discussion that *Cragun's* method calls for comparing a sum against a plurality of categories. Instead the "super" category appears to be an organizational feature with categories 808 being fit into a super category. Applicant requests that the rejection of claim 56 be withdrawn or that the Examiner provide further discussion or explanation of where *Cragun* teaches comparing a sum to a number of category thresholds prior to storing the data (rather than the single "log threshold" discussed in col. 4, lines 51-55).

C. Obviousness Rejections under 35 U.S.C. §103

Additionally, the Office Action rejected claims 1-4, 6-8, 12-15, 17-33, and 65-67 under 35 U.S.C. §103(a) as being unpatentable over U.S. Pat. No. 6,453,345 ("*Trcka*") in view of *Cragun* and U.S. Pat. No. 6,266,664 ("*Russell-Falla*"). This rejection is traversed based on the following remarks.

Claim 1 calls for "monitoring TCP/IP network communications" and "storing raw TCP/IP session data for said TCP/IP network communications on disk." Then, the stored communications are tested for a preselected criterion "wherein the raw TCP/IP session data including all TCP control and payload data is tested for the presence of the at least one preselected criterion." This process is discussed in Applicant's specification at least on page 4, beginning at line 11 where the method involves storing each TCP/IP half-session to a file or log and then searching the raw data "for the user-selected criterion." In other words, monitoring, searching, and communication storing is performed by processing TCP control information and TCP payloads or the actual user data together (e.g., processing a complete or whole captured network session rather than select processing of portions of network traffic).

Trcka is cited for teaching that the stored and tested information is "raw TCP/IP session data including all TCP control and payload data" that is tested for the presence of the criterion. Applicant disagrees with this understanding of *Trcka*. The Office Action cites *Trcka* at col. 6, lines 13-25, col. 7, lines 28-42, and col. 18, lines 15-29 for providing such teaching. However, *Trcka* describes a simple filtering mechanism (see, for example, col. 15, beginning at line 45). This filtering mechanism is applied to each data packet on an individual basis, and, as a result, **does not look for the presence of a preselected criterion in stored communications including raw TCP/IP session data including all TCP control AND payload data** and would produce a very different result than a testing process that looks at multiple packets or data payloads of a complete communication or session along with control data. In the last Amendment, Applicant discussed the fact that *Trcka* does not overcome the deficiencies of *Russell-Falla*. Specifically, it was argued that *Trcka* does not teach a user selecting a category, defining criterion for inspecting network communications, and does not show that the categories may have regular expressions. *Trcka* does not teach any specific type of analysis that would be performed on the raw data packets. Hence, *Trcka* does not teach the step of testing the stored communication for the presence of at least one user-defined criterion. In other words, *Trcka* needs to teach that all TCP control and payload data for a stored

communication is tested for at least one criterion, but it instead teaches a simple filtering of portions of a captured information. Turning specifically to the cited portions of *Trcka* at col. 17, line 56 to col. 18, line 14, the reference teaches filtering based on one of "(a) network address (source and destination), (b) traffic type, (c) packet type, (d) user ID, (e) field ID, and (f) packet transaction sequence." Each of these call for a search of a particular portion of a communication and do not call for testing the TCP control information and the payload data for one or more criterion. Hence, *Trcka* fails to teach the testing step of claim 1.

Claim 1 is amended to include the limitations of dependent claims 2-4 and 6-8, which are cancelled. In the Office Action, *Trcka* was said to fail to show the assigning of negative weights to regular expressions and that such negatively weighted expressions should be evaluated prior to positive weighted expressions in the same category. *Russell-Falla* was cited at col. 3, line 59 to col. 4, line 3 for teaching the assigning of negative weights, and Applicant agrees that this reference provides such teaching. However, Applicant strongly disagrees that the algorithm in col. 5, line 25 makes the evaluation of negative valued expressions "mathematically arbitrary" as to which values are evaluated first.

As discussed in the prior Amendment, Applicant's specification describes the process of looking for matches for negative values first (see, Figure 2 and related text) as this better controls false positives while also limiting the amount of processing required in the testing step to determine the presence of the preselected criterion (e.g., once a sum of the values/weights associated with the regular expressions equals or exceeds a threshold the criterion is determined to be satisfied or present in the stored communication – so, it is beneficial to process negatively weighted expressions first to reduce false positive results while still not requiring that all positively weighted expressions be processed). This is not a mere design choice or an obvious requirement, and it is only motivated by Applicant's specification as *Russell-Falla* teaches summing <u>all</u> weights for the matched expressions. Claim 1 is believed allowable because *Russell-Falla* fails to overcome this admitted deficiency of *Trcka*. *Cragun* is not cited for discussing the use of negative weights or of evaluating those with

negative weights first. The Response to Arguments section of the Office Action does not address the above argument.

Moreover, there is no teaching in the references as to how such a combination would be achieved of *Cragun* or *Russell-Falla* with *Trcka*. The references appear to teach against the combination suggested in the office action. For example, *Russell-Falla* deals with analyzing a web page before it is displayed whereas *Trcka* specifically captures data passively without interrupting delivery. *Russell-Falla* must analyze HTML pages, not network packets, whereas *Trcka* must capture network packets at a very low level. The two references, as taught in the references themselves, describe incompatible systems. Only Applicant has recognized and invented a way for performing text analysis akin to what *Russell-Falla* is doing on HTML pages in an offline manner within a network connection, akin to what *Trcka* is doing at a data link layer. Similarly, *Cragun* teaches the analysis of payloads, but its teaching does not mention that the method would be useful for a network traffic security system like *Trcka*'s system. Hence, Applicant requests that the Examiner provide motivation in *Trcka* or the other two references that there is a motivation to combine their teaching.

Claims 6, 12-15, 17-33, and 65-67 depend from claim 1 and are believed allowable over *Trcka*, *Cragun*, and *Russell-Falla* at least for the reasons provided for allowing claim 1. Further, claim 65 calls for testing to be performed "individually on each independent part." The Office Action cites *Trcka* at col. 18, lines 15-29 and at col. 7, lines 28-37 for teaching such testing of independent parts. At col. 18, lines 15-29, *Trcka* teaches that API 148 acts as an interface between databases and play-back devices to enable interpretation of traffic data such as to "display a web page or other HTTP-level transaction." There is no discussion of testing separate parts of the captured data. At col. 7, lines 28-37, *Trcka* teaches that its archival recording provides a complete replica of all valid network traffic and allows analysis of any transaction at any protocol level such as analysis at a network level or application level. However, there is no discussion a transaction has a plurality of independent parts such as a header, a message payload, an attachment to an e-mail, or the like that are to be

independently analyzed (let alone tested for criterion selected by a user). For this additional reason, claim 65 is believed allowable over *Trcka*.

Further, the Office Action rejected claims 9 and 10 under 35 U.S.C. §103(a) as being unpatentable over *Trcka* in view of *Cragun* and *Russell-Falla* as applied to claim 4 and further in view of U.S. Pat. No. 5,878,423 ("Anderson"). This rejection is traversed based on the following remarks. Claims 9 and 10 depend from claim 1 and are believed allowable over *Trcka*, *Cragun*, and *Russell-Falla* at least for the reasons provided for allowing claim 1. Anderson is not cited for overcoming the deficiencies of these three references discussed with reference to claim 1.

Yet further, the Office Action rejected claim 68 under 35 U.S.C. §103(a) as being unpatentable over *Trcka* in view of *Cragun* and *Russell-Falla* and in further view of U.S. Pat. No. 7,016,951 ("*Longworth*"). Claim 68 depends from claim 1 and is believed allowable over *Trcka*, *Cragun*, and *Russell-Falla* for the reasons discussed with regard to claim 1. *Longworth* is not cited for overcoming the deficiencies of these three references with reference to claim 1. Further, as discussed with reference to claim 65, *Trcka* fails to show testing of each independent part of stored TCP/IP network communications for user selected criterion. Hence, *Trcka*, *Cragun*, and *Russell-Falla* in combination with *Longworth* would not result in the claimed invention of claim 68.

Still further, the Office Action rejected claims 34-36, 42, and 44-54 under 35 U.S.C. §103(a) as being unpatentable over *Russell-Falla* in view of *Trcka* and *Cragun*. This rejection is respectfully traversed based on the following remarks.

Independent claim 34 includes "normalization" limitations similar to those found in claim 55 and, therefore, the reasons provided for allowing claim 55 over *Cragun* are applicable to claim 34. With regard to claim 34, though, the Office Action instead cites *Russell-Falla* for teaching the removing data content step (rather than *Cragun*). As discussed in the prior amendment, claim 34 calls for removing data content that does not contain language elements and then testing the "remaining content." The Office Action cites a portion of *Russell-Falla* that relates to scanning an HTML page for regular expressions. It appears that the entire HTML page is used as input for analysis, including non-language

elements. *Russell-Falla* does not show or suggest any activity of removing data content that does not contain language elements. At col. 5, lines 5-11, *Russell-Falla* is said to teach "the act of identifying and analyzing natural language elements," and the Examiner argues that this is within the scope of the removing data step of claim 34. However, such identifying does not indicate or teach that the other content was removed or that later the "remaining data" is to be stored (i.e., not the removed content). Hence, the removing data content step is not shown by *Russell-Falla*.

The Response to Arguments states that *Russell-Falla* "only tests the language elements" but there is no further citation to the reference of where it teaches "removing data content that does not contain language elements" and then "testing the remaining content." The Examiner simply argues that it is "clear" so, evidently, there must be a data content removing step, but Applicant could find no such teaching and respectfully requests that a citation showing such data content removal be provided for *Russell-Falla* or the rejection be withdrawn.

Additionally, claim 34 was amended to include the limitations of dependent claims 39 and 41, which call for the expressions to be weighted with negative or positive weights. These limitations are similar to those provided in claim 1, and the reasons provided for allowing claim 1 over *Trcka*, *Cragun*, and *Russell-Falla* are applicable to claim 34. Claim 34 also now calls for the testing and maintaining of sum values to be halted once a sum of values exceeds a user selected threshold value. Clearly, *Russell-Falla* does not show halting other processing steps once the sum meets or exceeds a user defined threshold as this reference shows summing all weights for matched expressions. By processing the negative results first, the halting of the process occurs at a different time, and evaluating negative weighted expressions first results in fewer false positives as discussed only by the Applicant in his specification (i.e., this is not an obvious design choice and no teaching to modify *Russell-Falla* was provided in that or the other references). The Office Action on page 15 fails to provide any citation for this limitation that is provided in the final wherein clause of claim 34. Hence, a *prima facie* case of obviousness has not been stated by

the Examiner for claim 34 (a mention of this limitation is provided at the bottom of page 16 but there is no citation to any of the references or indication that possibly the Examiner was taking Official Notice). For these additional reasons, claim 34 is believed in condition for allowance.

Further, as discussed in prior Amendments, *Russell-Falla* does not show or fairly suggest capturing data on a network comprising multiple half sessions of TCP/IP network communications. An HTML page comprises text data extracted from one or more TCP packets that are assembled at the browser according to the HTML rules. HTML is a markup language, not a protocol. Accordingly, an HTML page does not, by itself, define a "session" or "half session." An HTML page, like any computer file, may be delivered over a network communication protocol; however, the HTML page is itself entirely independent of any particular network communication protocol. Hence, an HTML page is by and intent design entirely unaware of any concept of "session" that exists on the network itself and so cannot satisfy the claim limitation "wherein the data comprises multiple half sessions..." appearing in claim 34.

The HTML page is distinct from a TCP/IP half session. Significantly, a TCP/IP (or other network level) communication typically includes a wide variety of non-HTML information. This data may include header information, cookies, parameter information, and the like. In some cases the network communication may include malicious (or benevolent) code or hidden data that "piggy backs" on the network communication packets used to deliver an HTML page. This is equally true of other applications such as email, instant messaging, and the like. This piggy-backed data is not a part of the HTML page in *Russell-Falla*, but it is a part of the captured half session in claim 34. Hence, this data will escape analysis in *Russell-Falla* but will be subject to monitoring by the invention of claim 34.

Claims 35, 36, 42 and 44-54, which depend from claim 34, are allowable for at least the same reasons as claim 34 set out above. Also, claims 52 and 54 are believed allowable for the additional reasons provided above for claims 31 and 33.

Finally, the Office Action rejects claims 62-64 under 35 U.S.C. §103(a) as being unpatentable over *Cragun* in view of *Trcka*. Claims 62-64 depend from claim 55 and are believed allowable over *Cragun* for the reasons provided for allowing claim 55 over that reference. *Trcka* is not cited for overcoming the deficiencies of *Cragun* discussed with reference to claim 55, and as a result, the combined teaching of *Cragun* and *Trcka* does not teach or suggest the method of claim 55.

D. Conclusion.

In view of all of the above, it is requested that a timely Notice of Allowance be issued in this case.

E. Petition for 2-Month Extension.

A Petition for 1-month extension was filed March 29, 2007 with the response to Final Office Action. The applicant hereby petitions for a 2-month extension to extend the due date for response an additional month from February 28, 2007 to April 29, 2007. Please charge an additional extension fee and other fee associated herewith to Deposit Account No. 50-1123. The Examiner is kindly asked to telephone the undersigned should any issues remain.

Respectfully submitted,

April 30, 2007

Carol W. Burton, Reg. No. 35,465
Hogan & Hartson L.L.P.
1200 17th Street, Suite 1500
Denver, CO 80202
Telephone: (303) 454-2454
Facsimile: (303) 899-7333